UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/798,578	03/12/2004	Yasuko Matsumura	31869-201591	6526

26694 7590 06/26/2007
VENABLE LLP
P.O. BOX 34385
WASHINGTON, DC 20043-9998

EXAMINER	
MORAN, RANDAL D	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
06/26/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/798,578	MATSUMURA ET AL.	
	Examiner	Art Unit	
	Randal D. Moran	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *3/13/2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19 and 29-35* is/are rejected.

7)☐ Claim(s) *20-28* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *3/13/2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *3/12/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The IDS filed on 3/12/2004 has been considered by the examiner.

2. Claims 1-35 are pending in the application.

3. Below, Examiner has pointed out particular references contained in the prior art(s) of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claims, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully each reference in its entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

Claim Objections

1. The following claims are objected to for lack of antecedent basis.
   - **Claim 9**- line 2, **Claim 16**- line 7, and **Claim 18**- line 3, recite the limitation "the member ID".

- **Claim 23**- line 11, **Claim 24**- line 10, recite the limitation "the secure channels".
- **Claim 26**- line 18, **Claim 27**- line 17, recite the limitation "the finite field".

Claim Rejections - 35 USC § 112

1. **Claims 1-35** rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

- Considering **Claim 1**- lines 8-10, it is unclear from the claim that only one second share is distributed to each member including one to the member that is generating the second shares. **Claim 1**- lines 11-15, it is unclear from the claim which share or which member is "the share generated by the member". For the purpose of examination, examiner interprets the claim to be: each member among the t members uses the secret sharing scheme to generate t second shares from its first share, and distributes one second share to each member including itself; each member among the t members performs a distributed computation by using the second share distributed to itself and the t-1 second shares received from the t-1 other members, the t members thereby generating t intermediate results.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. **Claims 1-8, 10-17, and 29-34** are rejected under 35 U.S.C. 102(e) as being anticipated by **Miyazaki et al. (US 6,810,122)**, hereafter "Miyazaki".

3. Considering **Claims 1, 10-12, and 29-31,** Miyazaki discloses s a shared secret reconstruction apparatus for reconstructing a secret in a secret sharing scheme that generates n first shares from the secret information (column 8- lines 15-23, Fig. 5), n being an integer equal to or greater than two (column 7- lines 64-67, column 8- lines 1-2), the n shares being distributed to a group having n members in such a way that the original secret information can be reconstructed by a collection of any t members (2 <= t <= n) separately possessing the shared secret reconstruction apparatus (column 9- lines 11-15), the shared secret reconstruction apparatus thus operating together with t-1 other shared secret reconstruction apparatuses (column 9- lines 3-10), the shared secret reconstruction apparatus comprising: a secret sharing operation unit generating

second shares from a first share held by the shared secret reconstruction apparatus by using a secret sharing scheme (column 9- lines 16-40) and distributing them to the t-1 other shared secret reconstruction apparatuses (column 9- lines 42-63); a secret reconstruction operation unit calculating an intermediate result for reconstructing the original secret information in a distributed computation by use of the output from the secret sharing operation unit and the second shares received from the t-1 other shared secret reconstruction apparatuses (column 9- lines 65-67; column 10- lines 1-12); and a secret reconstruction unit reconstructing the original secret information from the output from the secret reconstruction operation unit and the outputs received from the t-1 other shared secret reconstruction apparatuses (column 10- lines 61-67).

4. Considering **Claims 2, 13, and 34,** Miyazaki discloses the secret sharing scheme generates the n first shares in such a way that the original secret information is a sum of the n first shares (column 9- lines 3-15).

5. Considering **Claim 3, 4, and 14,** Miyazaki discloses the secret sharing scheme generates the second shares in such a way that a first share is a sum of all the second shares generated from the first share (column 10- lines 12-16).

6. Considering **Claims 5, 15, and 35,** Miyazaki discloses the n first shares are generated by a threshold secret sharing scheme using member IDs to identify each of the members (column 9- lines 43-64, column 10- lines 27-33).

7. Considering **Claims 6, 17 and 32,** Miyazaki discloses the second shares are generated from the first share held by each of the t members by using a threshold secret sharing scheme using member IDs (column 9- lines 43-64, column 10- lines 27-33) or by using a secret sharing scheme that can reconstruct the secret by summing all shares (column 9- lines 11-15, column 10- lines 12-16 and 61-67).

8. Considering **Claims 7 and 16,** Miyazaki discloses the shared secret reconstruction apparatus of claim 10, wherein the secret reconstruction operation unit comprises a linear combination operation unit performing a linear combination operation on the output from the secret sharing operation unit and the second shares received from the t-1 other shared secret reconstruction apparatuses using coefficients calculated from the member ID's (column 10- lines 1-16 and 27-67), the second shares being received via secure channels (it is inherent that in a secret sharing system data would be transmitted in a secure channel, abstract- lines 10-15).

9. Considering **Claims 8 and 33,** Miyazaki discloses a step of generating and distributing mutually distinct temporary member IDs to the t members (column 2- lines 1-16, column 8- lines 24-34), wherein: the intermediate results for reconstructing the original secret information are calculated by a distributed computation using the temporary member IDs (column 9- lines 43-67, column 10- lines 1-17, 27-33); and the original secret information is reconstructed from the intermediate results and the temporary member IDs (column 10 lines 12-16, 27-33, and 61-67).

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. **Claims 9, 18, and 19** are rejected under 35 U.S.C. 103(a) as being unpatentable over Miyazaki in view of **Knapp (US 2003/0046202)**, hereafter "Knapp".

3. Considering **Claims 9 and 18,** Mayaziki does not explicitly disclose a step of generating third shares from the member IDs of the t members by using a secret sharing scheme, and distributing them to the t members, the secret reconstruction operation unit thereby calculating an intermediate result for the

secret reconstruction in the distributed computation by use of the second and third shares output from the secret sharing operation unit and received from the t-1 other shared secret reconstruction apparatuses..

Knapp discloses a step of generating third shares from the member IDs of the t members by using a secret sharing scheme (Fig. 3, [0019] lines 14-34), and distributing them to the t members (Fig. 3, [0019] lines 14-34, [0022] lines 28-36).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Miyazaki by a step of generating third shares from the member IDs of the t members by using a secret sharing scheme, and distributing them to the t members, the secret reconstruction operation unit thereby calculating an intermediate result for the secret reconstruction in the distributed computation by use of the second and third shares output from the secret sharing operation unit and received from the t-1 other shared secret reconstruction apparatuses as taught by Knapp in order to minimize the chances that an adverse party, such as a hacker, is able to discover an entity's identification, the identification of any providers with whom the entity is dealing with or the identification of any digital products acquired by that entity (Knapp- [0019] lines 30-34).

The combination of Miyazaki and Knapp discloses the secret reconstruction operation unit thereby calculating an intermediate result for the secret reconstruction in the distributed computation (Miyazaki- column 9- lines 43-67, column 10- lines 1-17 and 27-33) by use of the second (Miyazaki- column 10- lines 15-16 and 32-33) and third shares (Knapp- Fig. 3, [0022]) output from the secret sharing operation unit and received from the t-1 other shared secret reconstruction apparatuses (Miyazaki- column 9- lines, 43-67, column 10- lines 1-17 and 27-33, Knapp- [0020] lines 5-17, [0022] lines 28-35) .

4. Considering **Claim 19,** the combination of Miyazaki and Knapp discloses a term calculation unit performing a distributed multiplication on the result of a distributed computation (Miyazaki- column 14- lines 47-54) performed on a coefficient calculated from the third share to the second share and on this second share by use of the second and third shares output from the secret sharing operation unit and received from the t-1 other shared secret reconstruction apparatuses (Miyazaki- column 14- lines 20-67, column 15- lines 1-15, Knapp- [0020] lines 5-17); and an adder summing all the outputs from the term calculation unit (Miyazaki- column 14- lines 55-67, column 15- lines 1-15).

Allowable Subject Matter

1. **Claims 20-28** are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

1. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- US 5,764,767 – System for reconstruction of a secret shared by a plurality of participants.
- PCT/US99/31053 – Re-splitting of shares in a secret sharing scheme.
- US 2003/021131 – Threshold sharing scheme using member ID's.
- US 2002/0012433 – Authentication using temporary ID's.
- US 6,463,154 – Managing use of temporary member ID's.
- US 2003/0088782 – Secret Sharing using biometrics.
- US 2006/0023887 – Threshold key sharing.

2. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Randal D. Moran whose telephone number is 571-270-1255. The examiner can normally be reached on M-F: 7:00 - 4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Randal D. Moran
/RDM/

6/5/07

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100